A class of symmetric controlled quantum operations

John A. Vaccaro, O. Steuernagel and S.F. Huelga
Division of Physics and Astronomy. Department of Physical Sciences,
University of Hertfordshire, Hatfield AL10 9AB, England
(February 1, 2008)

Certain quantum gates, such as the controlled-NOT gate, are symmetric in terms of the operation of the control system upon the target system and vice versa. However, no operational criteria yet exist for establishing whether or not a given quantum gate is symmetrical in this sense. We consider a restricted, yet broad, class of two-party controlled gate operations for which the gate transforms a reference state of the target into one of an orthogonal set of states. We show that for this class of gates it is possible to establish a simple necessary and sufficient condition for the gate operation to be symmetric.

I. INTRODUCTION

Quantum gates are the building blocks for quantum information hardware [1]. In particular, non-local quantum gates involving remote processors are the essential ingredients for performing distributed quantum computation [2] and implementing quantum communication protocols [3]. A given gate operation can be characterised in terms of how much entanglement it can create and how much classical information it can convey. This parameterisation establishes lower bounds in both the amount of entanglement and the classical communication resources that are required for the optimal implementation of a given quantum gate [4–7].

In this paper, we consider a particular class of controlled gates whose action is to transform a reference state of the target into one of a set of N orthogonal states. For clarity we shall call these gates *orthogonal gates*. They are generalisations of the controlled-NOT (CNOT) gate. Our aim is to provide an operational criteria which ensures *symmetric* operation of an orthogonal gate in the sense that the *control can be swapped with the target* for suitable preparation of the input states. Symmetric orthogonal gates allow the control system to communicate $\log_2 N$ bits of classical information to the target system and, because of their symmetry, allow for the same amount of reverse classical communication from target to control. By a suitable change of basis, they can also generate mutual entanglement between the states of the control and target systems. The orthogonality property ensures that an entanglement of $\log_2 N$ ebits can be generated in this way. Since there is a simple connection between the classical communication and the entanglement generated for symmetric orthogonal gates, we focus only on the classical information capability between two parties in this paper.

The main ideas underlying symmetric gates can be illustrated by considering a couple of specific gates. The CNOT gate is the simplest quantum gate. It is also a prime example of a symmetric gate: if Alice has the control qubit and Bob the target qubit, Alice can transmit one classical bit of information to Bob using the computational basis, and conversely Bob can transmit one classical bit of information to Alice using a Hadamard transformation of the computational basis [5,6].

The gate at the next level of sophistication is the controlled-Pauli (CP) gate [8]. This gate applies either the identity or one of the three Pauli-operators $\{\sigma_i : i = x, y, z\}$ on a target qubit depending on the state of two control qubits, and can be written as

$$U_{CP} = |00\rangle\langle 00| \otimes \mathbb{1} + |01\rangle\langle 01| \otimes \sigma_x + |10\rangle\langle 10| \otimes \sigma_y + |11\rangle\langle 11| \otimes \sigma_z.$$

Let Alice hold the control qubits and Bob the target qubit. Alice can transmit 2 classical bits of information per application of the CP gate using a variation of super-dense coding [9]. To see this consider the following protocol. Alice encodes a 2-bit message in binary notation using the basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ of her two qubits. Assume that Bob's qubit is in the (entangled) Bell state $|\phi^+\rangle = |00\rangle + |11\rangle$ with another qubit at his site. The CP gate is applied between Alice's particle and the first of Bob's particles. Depending on the state in which Alice has prepared her two control qubits, Bob will subsequently hold one of the four Bell states, which are mutually orthogonal. Therefore, he is able to infer Alice's message and thus receive 2 classical bits of information from Alice. We would like to know whether the gate is symmetrical from the point of view of its classical information capacity. In other words, *is it possible for Bob to choose certain initial states so that the gate operation results in two classical bits being conveyed to Alice?* If so, we would say that the gate is symmetric.

We can easily show that the CP gate can transmit one classical bit from Bob to Alice as follows. Consider the case when the first of Alice's qubits is kept in a fixed state, for instance in state $|0\rangle$. The action of a CP gate is now

equivalent to a controlled-NOT gate between Alice's second qubit and Bob's first qubit. Given that a controlled-NOT gate can transmit one classical bit in each direction [5,6], we know immediately that Bob can convey at least one classical bit to Alice. However we cannot be sure that certain initial preparation may allow Bob to actually transmit two classical bits using the CP gate. The aim of the paper is to remove this ambiguity for general orthogonal gates by providing an operational criteria for establishing the symmetry of this class of controlled gates.

The organisation of the remainder of the paper is as follows. We define orthogonal gates and present the conditions for symmetric orthogonal gates in Section II, we then apply the conditions to a number of different gates in Section III, we give proofs of the conditions in Section IV and we end with a discussion in Section V.

II. SYMMETRIC ORTHOGONAL GATES

A controlled quantum gate $\mathcal{G}$ allows Alice, using different orthogonal quantum states $|\psi_n\rangle_A$, to control the application of a set of unitary operations $\{U_n\}$ on Bob's particle's state $|\phi\rangle_B$. We call the gate's operation a *symmetric* controlled operation if it allows Bob to conversely control the state of Alice's particle to the same degree. As mentioned above, the CNOT is an example of a symmetric controlled gate with the controlled operations $\{U_n\}$ being the identity and the σ_x Pauli operator.

We restrict our attention here to the class of quantum gates for which the N controlled unitary operations $\{U_n\}$ operating on Bob's state space produce a set of N orthogonal states

$$\mathcal{N} = \{|n\rangle_B : {}_B\langle n|m\rangle_B = \delta_{n,m};\ n,m = 1,...,N\} \tag{1}$$

from a fixed reference state $|R\rangle_B$:

$$U_n|R\rangle_B = |n\rangle_B \text{ for } n = 1,\ldots,N \tag{2}$$

and so ${}_B\langle R|U_m^\dagger U_n|R\rangle_B = \delta_{m,n}$. We shall call such gates *orthogonal gates of cardinality* N. For clarity, we use subscripts A and B here, and subsequently, to distinguish the states of Alice's and Bob's particles, respectively. Note that we do not assume that $|R\rangle_B \in \mathcal{N}$ nor that $\mathbb{1} \in \{U_n\}$. Clearly the dimension of the state spaces of Alice's and Bob's particles must be at least N. For this paper we assume that the dimension of Bob's state space is *exactly* N. The (unitary) action of the gate $\mathcal{G}$ is hence assumed to be of the form

$$\mathcal{G}\left(|\psi\rangle_A|\phi\rangle_B\right) = \sum_{n=1}^{N} a_n |n\rangle_A U_n |\phi\rangle_B \tag{3}$$

$$= \sum_{n,m=1}^{N} a_n |n\rangle_A b_m U_n |m\rangle_B \tag{4}$$

where the input states are given by $|\psi\rangle_A = \sum_n a_n |n\rangle_A$ and $|\phi\rangle_B = \sum_n b_n |n\rangle_B$ with $\sum_n |a_n|^2 = \sum_n |b_n|^2 = 1$. Using Eqs. (2) and (4) it is easy to show that Alice can send one of N distinct messages to Bob in each application of the gate when the following input states are employed:

$$|\psi_n\rangle_A = |n\rangle_A,\ n = 1,...,N \quad \text{and} \quad |\phi\rangle_B = |R\rangle_B\ .$$

To be a symmetric gate, $\mathcal{G}$ must allow Bob to send one of N distinct messages to Alice per application of the gate for some suitable choice of input states. We prove the following equivalent Theorems in Section IV.

Theorem 1. A necessary and sufficient condition for symmetric operation of an orthogonal gate of cardinality N is that the set of pairwise products $\{U_n^\dagger U_m : n,m = 1,\ldots,N\}$ of the controlled operations U_n have the commuting property

$$(U_n^\dagger U_m)(U_p^\dagger U_q) = (U_p^\dagger U_q)(U_n^\dagger U_m)\ , \tag{5}$$

for $n,m,p,q = 1,...,N$.

Theorem 1′. A necessary and sufficient condition for symmetric operation of an orthogonal gate of cardinality N is that the set of controlled operators $\{U_n\}$ is related to a set of N commuting operators $\{C_n\}$ by

$$U_n = TC_n \text{ where } C_nC_m = C_mC_n \text{ for } n,m = 1,\ldots,N \tag{6}$$

and where T is unitary.

The latter version of the theorem is perhaps more transparent but, if T is not known, it is generally more straightforward to check the commuting property using Eq. (5). We note that if the set $\{U_n\}$ includes the identity then Eq. (5) implies the operators U_n must be mutually commuting. We shall also prove the following Theorem and Corollary regarding the structure of the states involved.

Theorem 2. Bob is able to send one of N distinct messages to Alice using a symmetric orthogonal gate of cardinality N iff the input state of Bob's particle is an eigenstate of the pairwise product $U_n^\dagger U_m$ [or, equivalently, an eigenstate of the operators C_n in Eq. (6)], and Alice's input state is $\frac{1}{\sqrt{N}}\sum_n e^{i\eta_n}|n\rangle_A$ for arbitrary, real η_n.

Corollary 3. The reference state $|R\rangle_B$ and basis set $\mathcal{N}$ in Eq. (2) for a symmetric orthogonal gate of cardinality N are given by

$$|R\rangle_B = \frac{1}{\sqrt{N}}\sum_{r=1}^{N} e^{-i\gamma_r}|\lambda_r\rangle_B \ , \tag{7}$$

$$|n\rangle_B = \frac{1}{\sqrt{N}}\sum_{r=1}^{N} e^{i[\varphi_n(r)-\gamma_r]}U_1|\lambda_r\rangle_B \ \text{ for } n=1,\ldots,N \tag{8}$$

where $e^{i\varphi_n(r)}$ and $|\lambda_r\rangle_B$ are the rth eigenvalue and eigenstate of the product $U_1^\dagger U_n$, and γ_r is an arbitrary, real parameter. Conversely, the eigenstates are given in terms of the $\mathcal{N}$-basis as

$$|\lambda_r\rangle_B = U_1^\dagger \frac{1}{\sqrt{N}} e^{i\gamma_r}\sum_{n=1}^{N} e^{-i\varphi_n(r)}|n\rangle_B \ \text{ for } r=1,\ldots,N \ . \tag{9}$$

Whereas Theorems 1 and 1′ are useful for deciding whether a particular orthogonal is symmetric or not, Theorem 2 and Corollary 3 are useful for constructing a symmetric orthogonal gate from a set of operators satisfying Eqs. (5) and (6).

III. APPLICATIONS

We illustrate the application of the Theorems and Corollary with a few examples. The simplest example is given for cardinality $N=2$, where N is the size of the set of controlled operators $\{U_n\}$. This occurs for the controlled-U gate where $\{U_n\}$ contains the identity $U_1=\mathbb{1}$ and another operator U_2. It is straightforward to show that this gate satisfies the orthogonal property Eq. (2) when $\mathcal{N}$ is the computational basis iff U_2 anticommutes with the operator σ_z. That is, U_2 is of the form

$$U_2 = e^{i\alpha}\begin{pmatrix} 0 & b \\ -b^* & 0 \end{pmatrix}$$

where α is real and $|b|^2=1$. The controlled-NOT, with $\alpha=0$ and $b=1$, is an example of this class. Since the set $\{U_n\}$ contains only two operators, one of which is the identity, the condition Eq. (5) is clearly satisfied. Hence all orthogonal controlled-U gates of cardinality 2 are symmetric.

Next consider the controlled-Pauli gate. In this case the set $\{U_n\}$ of controlled operators is given by $\{\mathbb{1}_1\otimes\mathbb{1}_2, \sigma_x\otimes\mathbb{1}_2, \sigma_y\otimes\mathbb{1}_2, \sigma_z\otimes\mathbb{1}_2\}$ and so the cardinality is $N=4$. Here $\mathbb{1}_i$ is the identity operator associated with Bob's ith qubit. This set fulfills the orthogonal property Eq. (2) when acting on the Bell state $|\phi^+\rangle_B$, as discussed in the Introduction, and so it is an orthogonal gate. But it fails to fulfill the condition Eq. (5) for all values of the indexes m,n,p,q and so the controlled Pauli gate is not a symmetric gate. This means that if Alice has the control, Bob *cannot* send 2 classical bits to Alice in one application of the gate. In the final Section, we determine the maximum amount of information Bob can actually send using this gate.

There are, however, symmetric orthogonal gates with cardinality $N=4$. One is given by the following set of commuting operators:

$$\begin{aligned}
C_1' &= |\lambda_1\rangle_B\,{}_B\langle\lambda_1| + |\lambda_2\rangle_B\,{}_B\langle\lambda_2| + |\lambda_3\rangle_B\,{}_B\langle\lambda_3| + |\lambda_4\rangle_B\,{}_B\langle\lambda_4| \\
C_2' &= |\lambda_1\rangle_B\,{}_B\langle\lambda_1| - |\lambda_2\rangle_B\,{}_B\langle\lambda_2| + |\lambda_3\rangle_B\,{}_B\langle\lambda_3| - |\lambda_4\rangle_B\,{}_B\langle\lambda_4| \\
C_3' &= |\lambda_1\rangle_B\,{}_B\langle\lambda_1| + |\lambda_2\rangle_B\,{}_B\langle\lambda_2| - |\lambda_3\rangle_B\,{}_B\langle\lambda_3| - |\lambda_4\rangle_B\,{}_B\langle\lambda_4| \\
C_4' &= |\lambda_1\rangle_B\,{}_B\langle\lambda_1| - |\lambda_2\rangle_B\,{}_B\langle\lambda_2| - |\lambda_3\rangle_B\,{}_B\langle\lambda_3| + |\lambda_4\rangle_B\,{}_B\langle\lambda_4|
\end{aligned}$$

for an arbitrary basis $\{|\lambda_n\rangle\}$. Eqs. (1) and (2) are satisfied for a suitable reference state, such as $|R\rangle_B = \frac{1}{2}\sum_n |\lambda_n\rangle_B$, constructed using Eq. (7). Also, one can easily show using Eq. (3) that for the input state $|\psi\rangle_A |\phi_r\rangle_B = \frac{1}{2}\sum_n |n\rangle_A |\lambda_r\rangle_B$ this gate produces one of four possible output states as follows

$$\mathcal{G}\left(|\psi\rangle_A |\phi\rangle_B\right) = \begin{cases} \frac{1}{2}(|1\rangle_A + |2\rangle_A + |3\rangle_A + |4\rangle_A)\,|1\rangle_B & \text{for } r=1 \\ \frac{1}{2}(|1\rangle_A - |2\rangle_A + |3\rangle_A - |4\rangle_A)\,|2\rangle_B & \text{for } r=2 \\ \frac{1}{2}(|1\rangle_A + |2\rangle_A - |3\rangle_A - |4\rangle_A)\,|3\rangle_B & \text{for } r=3 \\ \frac{1}{2}(|1\rangle_A - |2\rangle_A - |3\rangle_A + |4\rangle_A)\,|4\rangle_B & \text{for } r=4 \end{cases}$$

Alice can distinguish between the four possible final states of her particle because they are orthogonal, and so Bob can send 2 classical bits of information, per application of the gate, to Alice by his choice of input state $|\lambda_r\rangle_B$. The gate is therefore symmetric.

The simplest example of a symmetric orthogonal gate for arbitrary cardinality N is given by what we call the *controlled-shift gate* where the operation on the target is one of the family of N shift operators C''_n. The shift operators are defined as $C''_n \equiv \sum_{m=1}^{N} |(n-2+m)\mathrm{mod}N+1\rangle_B\,{}_B\langle m|$ for $n = 1,\ldots,N$. These operators produce a cyclic shift amongst the basis states $\mathcal{N}$ and clearly satisfy the orthogonal property Eq. (2) for arbitrary reference state $|R\rangle_B \in \mathcal{N}$. It is easy to show that the set of shift operators $\{C''_n\}$ satisfies the commuting condition Eq. (6) with $T = \mathbb{1}$ and so the controlled-shift gates are clearly symmetric orthogonal gates. Similarly, the related controlled-U gate which applies the unitary operation TC''_n, for some nontrivial unitary T, to the target particle is also a symmetric orthogonal gate.

IV. PROOFS

In this Section, we first prove the equivalence of the two Theorems 1 and 1′. We then give the proof of these Theorems by showing the sufficiency and necessity of the criteria Eq. (5) for symmetric operation. We end with proofs of Theorem 2 and Corollary 3.

Proof of equivalence. The commuting property Eq. (5) implies that the (unitary) products $U_n^\dagger U_m$ share the same set of N eigenvectors $\{|\lambda_n\rangle_B\}$. Consider the eigenvalue equation for the products $U_1^\dagger U_m$ for $m = 1,\ldots,N$ on the rth eigenvector [10]:

$$U_1^\dagger U_m\,|\lambda_r\rangle_B = e^{i\varphi_m(r)}\,|\lambda_r\rangle_B \ , \tag{10}$$

where the $\varphi_m(r)$ are real parameters with $\varphi_1(r) = 0$; rearranging gives

$$U_m\,|\lambda_r\rangle_B = e^{i\varphi_m(r)} U_1\,|\lambda_r\rangle_B \tag{11}$$

and hence

$$U_m = U_1 \sum_{r=1}^{N} e^{i\varphi_m(r)}\,|\lambda_r\rangle_B\,{}_B\langle\lambda_r| \ . \tag{12}$$

since the states $\{|\lambda_r\rangle_B\}$ form a complete orthonormal basis. We write $T = U_1\sum_n e^{-iw_r}\,|\lambda_r\rangle_B\,{}_B\langle\lambda_r|$ for arbitrary real w_r. Then

$$U_1 = T\sum_{r=1}^{N} e^{iw_r}\,|\lambda_r\rangle_B\,{}_B\langle\lambda_r|$$

and so from Eq. (12) we now have $U_m = TC_m$ where the C_m,

$$C_m = \sum_{r=1}^{N} e^{i[\varphi_m(r)+w_r]}\,|\lambda_r\rangle_B\,{}_B\langle\lambda_r| \ ,$$

form a set of N mutually-commuting operators. This shows that Eq. (6) follows from Eq. (5). The converse, that Eq. (5) follows from Eq. (6), is trivially true. This completes the proof of the equivalence of the two Theorems 1 and 1′.

Proof of Theorems 1 and 1′. The *sufficiency* of the commuting condition Eq. (5) is proved by showing that it allows Bob to generate one of N orthogonal output states of Alice's particle depending on the input state of his particle. Consider the trace of the product $U_n^\dagger U_m$ in the $\mathcal{N}$-basis Eq. (1):

$$\mathrm{tr}(U_n^\dagger U_m) = \mathrm{tr}(U_m U_n^\dagger) = \sum_{r=1}^{N} {}_B\langle r|\, U_m U_n^\dagger\, |r\rangle_B \ .$$

Using ${}_B\langle r|\, U_m U_n^\dagger\, |r\rangle_B = {}_B\langle R|\, U_r^\dagger U_m U_n^\dagger U_r\, |R\rangle_B$ from Eq. (2), $U_r^\dagger U_m U_n^\dagger U_r = U_n^\dagger U_r U_r^\dagger U_m$ from Eq. (5) and the unitarity property $U_r U_r^\dagger = \mathbb{1}$ gives

$$\mathrm{tr}(U_n^\dagger U_m) = \sum_{r=1}^{N} {}_B\big\langle R|U_n^\dagger U_m|R\big\rangle_B = \sum_{r=1}^{N} {}_B\langle n|m\rangle_B = N\delta_{n,m} \ . \tag{13}$$

However, calculating the trace in the eigenbasis $\{|\lambda_r\rangle_B\}$ given by Eq. (10) is found to give

$$\begin{aligned}\mathrm{tr}(U_n^\dagger U_m) &= \sum_{r=1}^{N} {}_B\langle \lambda_r|\, U_n^\dagger U_m\, |\lambda_r\rangle_B \\ &= \sum_{r=1}^{N} e^{i[\varphi_m(r)-\varphi_n(r)]}\end{aligned} \tag{14}$$

on use of Eq. (11). Equating Eq. (13) and Eq. (14) then yields

$$\delta_{n,m} = \frac{1}{N}\sum_{r=1}^{N} e^{i[\varphi_m(r)-\varphi_n(r)]} \ . \tag{15}$$

Consider the N-dimensional vector $\mathbf{v}(n)$ whose elements are given by $v_r(n) = e^{i\phi_n(r)}/\sqrt{N}$ for $r = 1, \ldots, N$. Eq. (15) shows that the set of vectors $\mathbf{v}(n)$ for $n = 1, \ldots, N$ form an orthonormal set, and so the matrix $\mathbf{M}$ whose columns are given by $\mathbf{v}(n)$ is unitary: $\mathbf{M}^\dagger\mathbf{M} = \mathbf{M}\mathbf{M}^\dagger = \mathbb{1}$. The expression $\mathbf{M}\mathbf{M}^\dagger = \mathbb{1}$ implies that

$$\delta_{r,r'} = \frac{1}{N}\sum_{n=1}^{N} e^{i[\varphi_n(r')-\varphi_n(r)]} \ . \tag{16}$$

We now choose the input states for Alice's and Bob's particles to be

$$|\psi\rangle_A\, |\phi_r\rangle_B = \frac{1}{\sqrt{N}}\sum_{n=1}^{N} e^{i\eta_n}\, |n\rangle_A\, |\lambda_r\rangle_B \tag{17}$$

for arbitrary, real parameters η_n. Using Eq. (11) we find that the output state of the gate will then be

$$\begin{aligned}\frac{1}{\sqrt{N}}\sum_{n=1}^{N} e^{i\eta_n}\, |n\rangle_A\, U_n\, |\lambda_r\rangle_B \ &= \frac{1}{\sqrt{N}}\sum_{n=1}^{N} e^{i\eta_n}\, |n\rangle_A\, e^{i\varphi_n(r)} U_1\, |\lambda_r\rangle_B \\ &= |\Psi_r\rangle_A\, |\Phi_r\rangle_B\end{aligned} \tag{18}$$

where

$$\begin{aligned}|\Psi_r\rangle_A \ &\equiv \frac{1}{\sqrt{N}}\sum_{n=1}^{N} e^{i[\varphi_n(r)+\eta_n]}\, |n\rangle_A \\ |\Phi_r\rangle_B \ &\equiv U_1\, |\lambda_r\rangle_B \ .\end{aligned}$$

The output states of Alice's particle $|\Psi_r\rangle_A$ are orthogonal over r according to Eq. (16),

$${}_A\langle \Psi_r|\Psi_{r'}\rangle_A = \frac{1}{N}\sum_{n=1}^{N} e^{i[\varphi_n(r')-\varphi_n(r)]} = \delta_{r,r'} \ . \tag{19}$$

Hence, provided Eq. (5) is satisfied, Bob can generate N different orthogonal states of Alice's particle. This completes the proof of sufficiency.

The *necessity* of the commuting condition is proved by beginning with the most general input state for Alice's particle, allowing Bob's particle to be in one of N orthogonal input states and then showing that for Alice's particle to end up in one of N orthogonal output states necessarily requires the commuting property Eq. (5). Let the input state be given by

$$|\psi\rangle_A |\phi_r\rangle_B = \sum_{n=1}^{N} a_n |n\rangle_A \sum_{m=1}^{N} b_m(r) |m\rangle_B \tag{20}$$

where $\sum_n |a_n|^2 = \sum_n |b_n(r)|^2 = 1$, and where the parameter r indicates that Bob chooses from some set of orthogonal states $\{|\phi_r\rangle_B\}$. In order that Alice be able to resolve the final state of her particle into different states indexed by r, without error, the output state of the gate must factorise into a product state. The combined output state $\mathcal{G}(|\psi\rangle_A |\phi_r\rangle_B)$ from Eq. (3) is therefore of the form

$$\sum_{n=1}^{N} a_n |n\rangle_A U_n |\phi_r\rangle_B = |\Psi_r\rangle_A |\Phi_r\rangle_B \tag{21}$$

where $|\Psi_r\rangle_A$ and $|\Phi_r\rangle_B$ are normalised states. The left-hand side factorises only if

$$U_n |\phi_r\rangle_B = \beta_n(r) e^{i\xi_n(r)} |\Phi_r\rangle_B \tag{22}$$

for all r, where $\beta_n(r) > 0$ and $\xi_n(r)$ are real parameters. Because of the unitarity of U_n this implies

$${}_B\langle\Phi_r|\Phi_{r'}\rangle_B \, \beta_n(r)\beta_n(r') e^{i[\xi_n(r') - \xi_n(r)]} = {}_B\langle\phi_r|\phi_{r'}\rangle_B = \delta_{r,r'}$$

and since ${}_B\langle\Phi_r|\Phi_r\rangle_B = 1$ then $\beta_n(r) = 1$. Both sets of input and output states $\{|\Phi_r\rangle_B\}$ and $\{|\phi_r\rangle_B\}$ therefore form complete orthonormal sets in Bob's state space and consequently there exists a fixed unitary mapping T' such that for all $r = 1, ..., N$

$$|\Phi_r\rangle_B = T' |\phi_r\rangle_B \ .$$

Together with $\beta_n(r) = 1$ and Eq. (22) this leads to

$$U_n = \sum_{r=1}^{N} e^{i\xi_n(r)} |\Phi_r\rangle_B \, {}_B\langle\phi_r| = T' \sum_{r=1}^{N} e^{i\xi_n(r)} |\phi_r\rangle_B \, {}_B\langle\phi_r| \ , \tag{23}$$

from which the commuting properties Eq. (5) and Eq. (6) follow. These commuting properties are therefore both sufficient and necessary for the symmetric operation. This completes the proof of Theorems 1 and 1′.

Proof of Theorem 2. Eq. (23) shows that Bob's input state $|\phi_r\rangle_B$ is necessarily an eigenstate of the pairwise products $U_n^\dagger U_m$ and so necessarily:

$$|\phi_r\rangle_B = |\lambda_r\rangle_B \tag{24}$$

where $|\lambda_r\rangle_B$ are defined in Eq. (10). Substituting this into Eq. (21) and using Eq. (11) shows that the output state of Alice's particle is necessarily

$$|\Psi_r\rangle_A = \sum_{n=1}^{N} a_n e^{i\varphi_n(r)} |n\rangle_A$$

up to an arbitrary phase factor. Alice must be able to distinguish N different output states indexed by r and so a necessary condition is

$${}_A\langle\Psi_{r'}|\Psi_r\rangle_A = \sum_{n=1}^{N} |a_n|^2 e^{i[\varphi_n(r) - \varphi_n(r')]} = \delta_{r,r'} \ .$$

Multiplying by $e^{-i\varphi_m(r)}$, summing over r and using Eq. (15) yields

$$|a_m|^2 N e^{-i\varphi_m(r')} = e^{-i\varphi_m(r')}$$

i.e. $a_m = e^{i\eta'_n}/\sqrt{N}$ where the η'_n are arbitrary, real parameters, and so a necessary condition for Alice's input state is that

$$|\psi\rangle_A = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} e^{i\eta'_n} |n\rangle_A \ . \tag{25}$$

Eqs. (17,18,19) show that Eq. (24) and Eq. (25) are also sufficient for Bob to send one of N distinct messages to Alice. Hence Theorem 2 is proved.

Proof of Corollary 3. Substituting Eq. (12) into Eq. (2) gives

$$U_n |R\rangle_B = U_1 \sum_{r=1}^{N} e^{i\varphi_n(r)} {}_B\langle\lambda_r|R\rangle_B |\lambda_r\rangle_B = |n\rangle_B \tag{26}$$

and hence, from the orthogonality of the sets $\{|n\rangle_B\}$ and $\{|\lambda_r\rangle_B\}$,

$$\delta_{n,m} = \sum_{r=1}^{N} e^{i[\varphi_n(r) - \varphi_m(r)]} |{}_B\langle\lambda_r|R\rangle_B|^2 \ .$$

Multiplying by $e^{-i\varphi_n(r')}$, summing over n and using Eq. (16) then gives

$$e^{-i\varphi_m(r')} = N e^{-i\varphi_m(r')} |{}_B\langle\lambda_{r'}|R\rangle_B|^2$$

and so

$${}_B\langle\lambda_r|R\rangle_B = \frac{1}{\sqrt{N}} e^{-i\gamma_r} \tag{27}$$

for arbitrary, real γ_r, which proves Eq. (7). Eq. (8) then follows from Eq. (26) and Eq. (27). Substituting Eq. (8) into the right-hand side of Eq. (9) and then performing the sum over n using Eq. (16) verifies the equality in Eq. (9).

V. DISCUSSION AND CONCLUSION

Up to now we have concentrated on symmetric orthogonal gates. We now discuss a result that applies to all orthogonal gates including those that are *asymmetric*. As before let Alice have the control of an orthogonal gate of cardinality N. Imagine a scenario where N_B is the number of classical messages (not necessarily the maximum) that Bob can choose to send to Alice and let the set of the N_B orthogonal input states that Bob uses for this be $\Lambda \equiv \{|\phi_r\rangle_B : r = 1, \ldots, N_B\}$. Further, let Bob choose to send the rth message and let Alice's input state be given, as before, by the general state $\sum_n a_n |n\rangle_A$. For Alice to be able to distinguish this message from all others, the output of the gate must factorise into the form given by Eq. (21). Eq. (22) then follows necessarily for $n \in \mathcal{R}$ where $\mathcal{R} \equiv \{n : a_n \neq 0\}$. This implies that

$$U_m^\dagger U_n |\phi_r\rangle_B = e^{i[\xi_n(r) - \xi_m(r)]} |\phi_r\rangle_B \tag{28}$$

for $n, m \in \mathcal{R}$ and $r = 1, \ldots, N_B$. The cardinality of the set $\mathcal{R}$ gives an upper bound on the dimension of the subspace in which the final state $\sum_n a_n e^{i\xi_n(r)} |n\rangle_A$ of Alice's particle lies, and hence must be at least N_B for Alice to be able to distinguish this many messages. We note that the operator products on the left-hand side of Eq. (28) could share more eigenstates than the N_B states in Λ. Thus a *necessary* condition for Bob to send N_B messages to Alice is that the set $\mathcal{R}$ must contain at least N_B elements and all the elements in $\{U_m^\dagger U_n : n, m \in \mathcal{R}\}$ must share at least N_B eigenstates.

We have already shown that a controlled-Pauli gate is asymmetric and that Bob cannot send 2 bits of classical information to Alice per application of the gate if Alice has the control qubits. Armed with this necessary condition we can now determine just how much classical information Bob can transmit to Alice. For Bob to be able to send 1 of 3 distinct messages, the set $\mathcal{R}$ must contain at least 3 elements and all the elements in $\{U_m^\dagger U_n : n, m \in \mathcal{R}\}$ must share at least 3 eigenstates. It is easy to show that this necessary condition is not fulfilled for the operators $U_n \in \{\mathbb{1}_1 \otimes \mathbb{1}_2, \sigma_x \otimes \mathbb{1}_2, \sigma_y \otimes \mathbb{1}_2, \sigma_z \otimes \mathbb{1}_2\}$ of the controlled-Pauli gate. Hence Bob cannot send 1 choice from 3 distinct

messages. In the Introduction we gave a protocol that allows Bob to send 1 choice from 2 distinct messages to Alice. This is therefore the *maximum* he can send. Thus Bob is limited to sending only one bit of classical information back to Alice as opposed to the two bits she could send.

In conclusion, we have defined a class of controlled quantum gates, which we call orthogonal gates, obeying the property Eq. (2). We investigated the algebraic structure that makes these gates symmetric with respect to the interchange of the control and target systems. We have shown that all such gates obey the commuting properties Eq. (5) and Eq. (6) and that these properties are sufficient. We also discussed a necessary condition that is useful for determining the maximum number of classical messages able to be sent using asymmetric orthogonal gates. We hope that this initial research may shed light onto the more general problem of establishing the classical communication capacity of general, not necessarily controlled, multiparty quantum gates.

Acknowledgements. The authors thank A. Chefles, P. Papadopoulos and M.B. Plenio for discussions. This work has been supported by the Engineering and Physical Sciences Research Council (EPSRC) and DGICYT Project No. PB-98-0191 (Spain).

---

[1] A. Barenco et al, Phys. Rev. A**52**, 3457 (1995).
[2] J.I. Cirac, A.K. Ekert, S.F. Huelga and C. Macchiavello, Phys. Rev. A**59**, 4249 (1999).
[3] J.I. Cirac et al, Phys. Rev. Lett. **78**, 3221 (1997). S.J. van Enk, J.I. Cirac and P. Zoller, Science **279**, 205 (1998). H.J. Briegel et al. Phys. Rev. Lett. **26**, 5932 (1998).
[4] A. Chefles, C. R. Gilson and S. M. Barnett, 'Entanglement, Information and Multiparticle Quantum Operations', quant-ph/0003062.
[5] J. Eisert, K. Jacobs, P. Papadopoulos and M.B. Plenio, Phys. Rev. A**62**, 052317 (2000).
[6] D. Collins, N. Linden and S. Popescu, 'The non-local content of quantum operations', quant-ph/0005102.
[7] J. I. Cirac, W. Dür, B. Kraus and M. Lewenstein, 'Entangling operations and their implementation using a small amount of entanglement', quant-ph/0007057.
[8] M.B. Plenio invented this gate for the discussion of the minimal resources required for the remote implementation of an arbitrary unitary operation. (See S.F. Huelga et al, quant-ph/0005061).
[9] C.H. Bennett and S.J. Wieser, Phys. Rev. Lett. **69**, 2881, (1992).
[10] The analysis is easily extended to the general products $U_n^\dagger U_m$ for an arbitrary value of n, but, for clarity, we treat $n = 1$ here.